E-FILED
Tuesday, 20 October, 2009 02:08:03 PM
Clerk, U.S. District Court, ILCD

EXHIBIT 67

Case Information United States v. Ali Saleh Kahlah Al-Marri

Lab# 2009-0711

08/13/2009

Case Number	**2009-0711**
Case Description	Examination of the image files of a 20Gb hard drive which had been contained in a Toshiba S3000-400 laptop computer, Model# PS300E-03YNL-G3, SN# 71824452G, belonging to Ali Al-Marri. The actual drive is sealed as evidence by and in the possession of the government for the prosecution of Mr. Al-Marri. The purpose of the examination was to ascertain if claims by the FBI examiner are in fact supported by the facts.
Report Created	Thursday August 13, 2009

Examination Details

On the morning of Saturday, July 11, 2009, I met with Andrew and Cheryl Savage, who are part of the team of attorneys for Mr. Al Marri to discuss the case and receive a copy of the government produced forensic images of the hard drive from Al Marri's computer. The images were furnished to me on a Western Digital 80Gb hard drive.

Once I arrived back at my lab, I proceeded to mount the images with FKT Imager, in order to have a quick look at the file system and other system data. It was readily apparent that this was not a true copy of the original drive. The image files were of an 80Gb drive that appeared to have the original 20Gb hard drive cloned onto it. That drive had been placed into a computer and booted. While booted, the user had explored the drive briefly, and then imaged that onto a drive that we were furnished. This was evident by the size difference of the drives involved, the creation of new files, and the modification and access of files that were already on the disk.

I saw no evidence that this was an attempt to deceive anyone, and was merely the result of not using best practices. We were later furnished a true copy, and this seemed to be born out.

Mr. Al-Marri's drive was a 20Gb drive, which had been partitioned with one primary and one extended partition and formatted FAT32. The installed operating system was WinME, and had been installed 10-31-01 and had been successfully booted 3 times prior to seizure. The computer was set up to allow the operator to boot either to WinME (English version) or WinME (Arabic version), however when the operator chose the Arabic version, it was in fact an English language version. The primary partition was the bootable partition and the extended partition appeared to be intended for storage.

There are indications that the OS had been re-installed and this is in fact confirmed by Al-Marri, after he had many problems with it. He did this in an attempt to overcome the "blue screen of death" as it commonly referred to which is what occurs when a

Windows based operating system is corrupt. There is no evidence the drive had been "wiped", or overwritten. This is a process one would use to try and eliminate any residual data from a drive. There were in fact over 27 thousand files that had been deleted but still recoverable, and an additional 33 thousand plus files that were recovered using file carving scripts in FTK (Forensic ToolKit) which is one of the same forensic software programs the government examiner used.

There were at least 2 programs installed on the computer to provide internet protection, Symantec and Zone Alarm with no exclusions chosen. These programs would effectively kill any programs one attempted to install and execute in order to attempt hacking. The installed OS is not one would chose for any activities such as this due to the limited command line function available to the operator and it's inability to see and control other operating systems such as would be found in many servers. There were still numerous instances of Trojan programs and viruses throughout the disk. A truly knowledgeable computer user would know that to eliminate these problems completely, the drive would have to be wiped completely, and this had not been done.

While there were many installation files located on the storage partition, there was no evidence that any of those files had been actually installed on the system. If there were there would in all likelihood be remnants found in the operating system and there were none found after scanning the drive with Gargoyle by Wetstone. Gargoyle is a program designed to detect the presence of malware on a system.

The government alleges that Al-Marri was searching on the internet for various dangerous chemicals, but does not say when. The government report has only found 1 such attempt for Sodium Cyanide, and the resulting "Excite" search results page. There is no finding that all these sites were visited as one might be expected to do. The additional search hits the government offers are in fact remnants of one MSDS (Material Data Safety Sheet) which is required by our own government regulations to be attached to dangerous chemicals. No indication was found of attempts to contact any of the sites visited. There is no evidence of instructions on how to mix or use the chemicals for any sinister purpose. As this information was found in unallocated space on the computer there were no dates found for the files because they were only fragments of files. The only date found within any of the recovered material was an embedded date of 6-12-01, at 9:18PM on the Potassium Cyanide hit. This appears to be the date the web page was last updated.

Mr. Al-Marri did in fact visit several weapons sites but there is no indication he searched for anything in particular.

The terrorist images found on the computer are the same that one would expect to find on almost any computer on the internet during that time period, and were almost all thumbnail size, found in temporary internet files. This is indicative of them being displayed on a webpage such as CNN.com etc.

The government puts great stock in the fact that Al-Marri used what is known as an "anonomyzer" program on his computer and gives the impression he used it only when visiting certain specific sites. The fact is, there is such a program installed on his computer, but it was used at all times the computer was on the internet by Al-Marri. This program does not erase his activities; it only makes the user appear to be coming from somewhere else to the site visited.

The email addresses and emails the government lists to show terrorist activities are in fact there. Not being fluent in the Arabic language and not knowing specific interactions between the parties involved, I can only confirm their presence.

Similarly, the audio files listed by the government are there, but again, not knowing Arabic I can only confirm their presence.

There are programs located on the computer that can be used to generate credit card numbers, and there appears to be attempts by Al-Marri to use them, but only to purchase pre-paid calling cards in relatively small denominations.

Forensic Examiner	Bill Capps, CFCE, ACE
Agency	Digital Data Recovery
Address	2961 Duren Ct. Charleston, SC 29414
Phone	843-813-0956
Fax	843-766-2891
E-mail	Bill@Digital-Data-Recovery.net

Conclusions

While the government has made many claims against Mr. Al-Marri, a thorough forensic examination of his computer cannot fully support the charges made against him. While there is some minor amount of data present on the drive in the categories claimed by the government, there is simply not enough there to give rise to more than speculation and conjecture.